Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls	)	

COMMENTS OF MICROSOFT CORPORATION

TABLE OF CONTENTS

SUMMARY

- The battle against tech support scams and other forms of caller ID fraud demands a multi-pronged effort and coordination by a variety of stakeholders domestically and internationally.
- Call blocking can be an effective tool in combating illegal robocalls and caller ID fraud, but the practice should be used minimally and rules governing it should be carefully tailored to prevent harm to network reliability and consumer welfare.
- Imprecise anti-robocalling efforts resulted in one carrier blocking 1.2 million SkypeOut calls in the U.S. over a four-month period earlier this year.
- A telephone number is not needed to place an outgoing call to the public switched telephone network. Several applications that permit outbound calls to the public switched telephone network from an internet-connected device do not assign a telephone number to the calling party. If these applications are not considered during the development of rules designed to prevent caller ID fraud and illegal robocalls, such non-traditional calling applications and their underlying technology may inadvertently be swept into the category of blocked calls.
- The FCC should encourage and explore methods other than call blocking to reduce the harms caused by caller ID fraud and illegal robocalling.
- The entity to which the spoofed number is validly assigned should have control over how their telephone number is used, including the ability to prevent unauthorized spoofing through a request for originating number blocking. The Commission should institute additional measures relating to this authorization.
- Subscriber notice and consent should be required before blocking of already-originated, incoming calls is authorized.
- The Commission should ensure that it does not inadvertently authorize blocking of international calls from non-NANP telephone numbers.
- The Commission should not authorize blocking of numbers that have not been assigned to a subscriber because it is not feasible at this time and because many legitimate calls utilize unassigned numbers for caller ID.
- Microsoft has concerns with the current form of SHAKEN but believes that it holds promise, although it is not ready for implementation or review and approval by the Commission.
- The Commission should refrain from instituting safe harbors at this time. Refraining to institute safe harbors will incentivize precision in authorized call

blocking. Nevertheless, in recognition of the fact that implementation of the rules may involve some industry-wide learning, the Commission should exercise prosecutorial discretion and avoid taking unnecessarily aggressive enforcement actions during the early months against good-faith efforts to implement the rules.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	

COMMENTS OF MICROSOFT CORPORATION

Microsoft maintains a unique position in this proceeding.[1] Microsoft and its customers have the potential of being harmed by those engaged in caller ID fraud and illegal robocalling, and thus Microsoft has a strong interest in eliminating or reducing those practices. At the same time, Microsoft's Skype product and Skype customers have the potential of being harmed – indeed, have been harmed – by overzealous or poorly executed, albeit well-intentioned, anti-robocalling efforts. Thus, Microsoft would like to constructively assist in the industry effort to establish rules and practices to combat caller ID fraud and illegal robocalls in ways that do not harm legitimate calls, including those made using non-traditional voice technologies.

[1] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Notice of Proposed Rulemaking and Notice of Inquiry, FCC 17-24 (rel. Mar. 23, 2017) ("Notice").

I. Successfully Combating Tech Support Scams and Similar Fraud Requires a Multi-Pronged Approach

Most participants in this proceeding are likely aware of tech support scams. It is such a common phenomenon that 66 percent of people have encountered a tech support scam attempt in the past year.[2] Microsoft receives an average of 10,000 complaints a month from consumers across the globe relating to these scams, and those are just the people who have taken the time and initiative to report the scam to Microsoft. Typically, these scams are perpetrated by fraudsters who pretend to be a technology company (such as Microsoft) and contact individuals with a fabricated claim of a technological vulnerability in their device or software that must be resolved. In their early form, the initial contact would tend to take the form of a "cold call" to a consumer's telephone number and sometimes involved fraudulently modifying the caller ID so that the call appeared to come from a familiar technology company. This method of fraud has morphed more recently such that the initial contact also can take the form of a computer screen pop-up, such as the one pasted below, identifying a

[2] This figure comes from an international survey commissioned last year by Microsoft and conducted by Ipsos Public Affairs. More information is available at: <https://mscorpmedia.azureedge.net/mscorpmedia/2016/10/10.17-Methodology.pdf> and at: <https://blogs.microsoft.com/on-the-issues/2016/10/17/tech-support-scams-growing-problem/#sm.0001el20x2191qf2dwnrwxckmqxzd>.

fabricated vulnerability, and providing a telephone number for the customer to call to resolve this artificial danger.

The fraudsters then induce the customer to purchase online technical support that is not actually needed. In addition, some scammers will charge credit cards or bank accounts for more than they were authorized to charge. They may also install malware on a victim's device, enabling ongoing access to the computer. Finally, fraudsters obtain online access to the customer's computer, making it possible to view and extract personal and confidential information.

Reasonable FCC actions are welcomed and warranted and can play an important role in combating fraud. The FCC, however, does not nor cannot shoulder this burden

alone. To be effective, the battle against tech support scams and other incidents of caller ID fraud demands a multi-pronged effort and coordination by a variety of stakeholders domestically and internationally.

For example, combating these scams requires consumer education so that customers can better understand the tell-tale signs of a scam and can adopt best practices when interacting with unknown third parties and allowing access to their devices or information.[3]

In addition, law enforcement must actively pursue criminals and, wherever possible, coordinate across jurisdictions and agencies. In the United States, the Federal Trade Commission and the Department of Justice have engaged in multi-jurisdictional

[3] For example, Microsoft provides these tips for consumers to follow if they receive a notification or call from someone claiming to be from a reputable software company: (1) Be wary of any unsolicited phone call or pop-up message on your device; (2) Microsoft will never proactively reach out to you to provide unsolicited PC or technical support; (3) Any communication Microsoft has with a consumer must be initiated by the consumer; (4) Do not call the number in a pop-up window on your device. Microsoft's error and warning messages never include a phone number; (5) Never give control of your computer to a third party unless you can confirm that it is a legitimate representative of a computer support team with whom you are already a customer; and (6) If skeptical, take the person's information down and immediately report it to your local authorities.

enforcement actions to combat this form of fraud.[4] Microsoft also supports efforts to crack down on tech support scams in other countries around the world.[5]

Technological tools also play a role in reducing the vulnerability of devices to viruses and/or their susceptibility to fraudulent pop-ups or advertisements. For example, the SmartScreen filter, which is built into Windows, Microsoft Edge browser, and Internet Explorer browser, helps to protect against malicious websites and downloads, including many of the pop-up windows. In addition, Bing blocked more than 17 million fraudulent tech support ads last year. Further, as described below, Microsoft is innovating on alternative technological approaches to protecting consumers from caller ID fraud.

---

[4] *See* a summary of recent enforcement actions against tech support scams at <https://www.ftc.gov/system/files/attachments/press-releases/ftc-federal-state-international-partners-announce-major-crackdown-tech-support-scams/operation_tech_trap_chart_of_actions.pdf>. *See also* "The Fight Against Tech Support Scams," by Courtney Gregoire, Assistant General Counsel, Microsoft Digital Crimes Unit (May 18, 2017), *available at* <https://blogs.microsoft.com/on-the-issues/2017/05/18/fight-tech-support-scams/#sm.00017peh8lpttcs2wqj1h88kryeal>.

[5] For example, in addition to directly referring cases, Microsoft India supported cybercrime training for more than 385 law enforcement officers and over 400 prosecutors in India in the past year. Last week, four fraudsters were arrested in the UK after two years of forensic and investigative work by the City of London Police and Microsoft. For more information, please visit: <https://news.microsoft.com/en-gb/2017/06/28/four-arrested-police-work-microsoft-crack-fraudsters/#sm.00017peh8lpttcs2wqj1h88kryeal>.

Finally, the telephone network itself can be managed in a way that will minimize opportunities for fraud. The Robocall Strike Force, ATIS, and the FCC are uniquely positioned to focus on network-based mechanisms and the Notice contains several proposals for this prong.

II. Network-Based Methods of Combating Caller ID Fraud Should Minimize Call Blocking

Call blocking is an extreme mechanism for combating illegal robocalls and caller ID fraud. Unless executed with complete precision, which is difficult to attain, call blocking mechanisms will inadvertently prevent legitimate calls from being completed, thereby reducing the utility and reliability of the public switched telephone network. In extreme circumstances, one could conceive of calls that are blocked that could have severe consequences for the safety of life and property. Imagine a child in danger calling a parent for help from an unfamiliar phone only to have their call blocked because it is mistaken as an illegal robocall. The stakes are high when voice providers block calls versus implementing alternative approaches, such as warning their customers that they perceive irregularities, thus putting the customer on notice.

Recent efforts to reduce illegal robocalls have led to large-scale blocking of legitimate calls in recent months. Between November 2016 and February 2017, a major U.S. carrier blocked more than 1.2 million SkypeOut calls under the misperception that they constituted illegal robocalls. Eventually, this matter was resolved and the carrier stopped the practice that prevented the completion of legitimate calls, but only after 1.2

million calls failed over a four-month period. That is not an acceptable way for the nation's telephone system to operate.

The Notice acknowledges the Commission's history of characterizing call blocking as potentially impairing network reliability and generally inconsistent with the obligations in section 201 of the Communications Act.[6] The Commission has permitted common carriers to block certain calls or categories of calls, but only upon instruction from their subscribers, and almost never unilaterally. For example, many carriers offer programs allowing customers to prevent their phone from ringing for calls lacking caller ID. In these cases, however, the circumstances in which calls should be blocked are somewhat straightforward; the absence of caller ID is an unambiguous characteristic and easy to determine with precision. By contrast, identifying a call as a robocall or one that is engaged in caller ID fraud involves greater ambiguity and, hence, a higher potential for error. Accordingly, while the Commission should continue to promote lawful efforts

[6] *See* Notice at ¶ 9 ("Because call blocking poses a threat to the ubiquity and seamlessness of the network, the Commission has long had a strong policy against allowing voice service providers to block calls."); *see id.* at n.31 ("The Commission has previously found call blocking, with limited exceptions, is an unjust and unreasonable practice under section 201(b) of the Act.") (citations omitted); s*ee also Establishing Just and Reasonable Rates for Local Exchange Carriers, Call Blocking by Carriers*, Declaratory Ruling and Order, 22 FCC Rcd 11629, ¶ 7 (WCB 2007) ("except in rare circumstances [the FCC] does not allow carriers to engage in call blocking"); *see also Policies and Rules Concerning Operator Service Providers*, Declaratory Ruling and Order, 28 FCC Rcd 13913, ¶ 9 (WCB 2013) ("The Commission has allowed call blocking 'only under rare and limited circumstances.'") (citation omitted).

to reduce caller ID fraud and robocalling, any mechanisms to do so that involve call blocking should be narrowly and carefully tailored.

Careful tailoring requires precision in identifying the types of call that may be blocked, and under what circumstances. Caller ID spoofing is neither unlawful nor inherently suspicious. The Truth in Caller ID Act (incorporated into the Communications Act) renders caller ID spoofing unlawful only when it is accompanied by a level of scienter: the intent to defraud, cause harm, or wrongfully obtain anything of value.[7] By adopting this measured approach, Congress wisely recognized that caller ID spoofing can be legitimate and harmless. The FCC acknowledges likewise:

> [T]here are legitimate uses for spoofing, such as a domestic violence shelter seeking to protect victims who make calls, doctors wanting to display their main office number, or call centers calling on behalf of a business displaying that business' main customer service number or a toll-free number for return calls instead of the number for the originating line used by the call center. [8]

Hence, it is overbroad to state that "blocking a call from a spoofed number is not, by definition, an unjust or unreasonable practice or unjustly or unreasonably discriminatory

[7] 47 U.S.C. § 227(e)(1) ("It shall be unlawful for any person within the United States, in connection with any telecommunications service or IP-enabled voice service, to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value, unless such transmission is exempted pursuant to paragraph (3)(B).").

[8] Notice at ¶ 5.

practice."[9] In fact, caller ID spoofing writ large has not been determined to be an unjust or unreasonable practice, whereas call blocking has repeatedly been found to be unjust and unreasonable.[10] If the Commission were to adopt the Notice's overbroad conclusion, it would exceed the scope of the directive in the Truth in Caller ID Act and would be inconsistent with the Commission's acknowledgement that some types of spoofing should be preserved. Accordingly, the Commission should carefully tailor its conclusion to specify that any unreasonableness relating to caller ID spoofing is premised upon the intent of the spoofing party, and not the act of spoofing itself.

A. *Subscribers Should be Permitted to Block Origination of Calls from Numbers Assigned to Them*

Microsoft supports the Commission's proposal, set forth in proposed rule sections 64.1200(k)(1) and (3), to allow a subscriber to block calls made from an originating number assigned to that subscriber. The entity to which the spoofed number is validly assigned should have control over how their telephone number is used, including the ability to prevent unauthorized spoofing through a request for originating number blocking.

In conjunction with finalizing the rule, the Commission should consider and adopt additional measures. For example, the Commission should instruct industry to

[9] *Id.* at ¶ 12.

[10] *See, e.g., id.* at n.31.

develop a robust method of reversing an originating number block so that if a number is re-assigned to another user, there is no interference in the new user's ability to complete outgoing calls. If originating number blocking is managed by the provider to which the number was allocated, a system should be developed to support the customer request (or not) in the event of number porting. That system should be reviewed and approved by the Commission.[11]

B. *The Commission's Rules Should Require Subscriber Notification and Consent Before Any Type of Call Blocking Is Instituted*

Subscriber consent must, of course, be obtained from the subscriber to the originating number prior to blocking calls from the originating number. For other call blocking mechanisms, subscriber notice and consent should be required before blocking of already-originated, incoming calls is deemed to be authorized. The Notice proposes to eliminate consumer notice and consent and to allow unilateral call blocking by carriers to avoid "unnecessary burden" or for technical infeasibility, without specifying how notifying customers and obtaining their consent would be burdensome or

[11] If sharing of such a request among carriers is warranted and permissible, the Notice does not indicate whether an originating number blocking mechanism requires a dip to a joint database and, if so, who would have access to such database, who pays for it, who is responsible for correcting erroneous block orders, how that correction would occur, and within what period of time the correction must be completed to enable a legitimate user to make outgoing calls using the number. Clarification of such matters would facilitate an orderly, consistent, and industry-wide implementation of the proposal.

technically infeasible.[12] Notifying subscribers and obtaining their consent is important as a matter of law, consumer protection, and network reliability.

To allow a carrier to block a call without notifying and obtaining the consent of the called party would constitute a radical departure from the common carrier principles that have formed the foundation of the public switched telephone network since the inception of regulation. The hallmark of authorized call blocking has consistently been the presence of consumer notice and consent. The Commission has emphasized the importance of consumer notice and consent, and expressed grave concerns about carriers blocking calls "at their own discretion without providing consumers any choice or, indeed, even awareness of the practice."[13]

Further, from a practical commercial perspective, telephone service subscribers pay for connectivity, including the ability to receive calls placed to their telephone number. If that connectivity is going to be routinely and deliberately deprecated, even for their benefit, subscribers should be informed of that fact, and be given the option to choose whether or not to permit filtering of their incoming calls.

[12] Notice at ¶ 25.

[13] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et al.,* Declaratory Ruling and Order, 30 FCC Rcd 7961, ¶ 158 (2015).

The importance of subscriber notice and consent is underscored by the potential for error. Unless carriers can guarantee 100 percent accuracy of call blocking mechanisms, there remains an undeniable risk that legitimate calls – perhaps urgent or important calls – will not be delivered to subscribers.[14] Under such conditions, and without notice and consent, consumers could remain unaware of the probability that some legitimate callers will be unable to reach them, they will lack the ability to identify white-listed numbers, and they will lack the option to decline blocking so that they receive all incoming calls. In short, subscriber notice and consent helps to ensure robust network reliability and usability for consumers.

C. *The Commission Should Clarify That International Calls Cannot Be Blocked on the Basis That They Do Not Originate From North American Numbering Plan Numbers*

Proposed rule section 64.1200(k)(2)(i), as currently drafted, proposes that "[p]roviders may block calls originating from . . . a number that is not a valid North American Numbering Plan number." It seems unlikely that the Commission intends to allow blocking of nearly all international calls, yet the wording of the proposed rule could do just that since calls from most other parts of the world originate from numbers that are not valid NANP numbers. The public switched telephone network's global reach is one of its strongest features. The Commission should avoid any imprecision in

[14] The Notice does not and should not suggest that it would be reasonable for carriers to block legitimate calls without consumer notice and consent.

its rules that would permit that feature of the network to be degraded. Accordingly, the Commission should decline to adopt proposed section 64.1200(k)(2)(i) or should modify it to avoid inadvertently authorizing international call blocking.

In addition, the Notice asks whether an internationally originated call purportedly originated from a NANP number should be subject to these rules.[15] Some legitimate internationally originated calls may utilize, for caller ID purposes, a valid NANP number that has been allocated to a provider but not assigned to an individual consumer, particularly if those calls originated abroad on the internet and entered the public switched telephone network in the United States. Accordingly, the Commission should specify that its rules are not intended to permit blocking of internationally originated calls that utilize valid NANP numbers for caller ID.

D. *The Commission Should Not Permit Blocking of Calls from Numbers That Have Not Been Assigned to a Subscriber*

The Commission should reject proposed section 64.1200(k)(2)(iii).[16] It would permit voice service providers to block calls that had been allocated to a provider but not assigned to a subscriber. Microsoft is unaware of a database accessible industry-wide that operates in real-time and with reliability sufficient to identify when a provider

[15] Notice at ¶ 24.

[16] "Providers may block calls originating from . . . a valid North American Numbering Plan number that is allocated to a provider by the North American Numbering Plan Administrator or Pooling Administrator, but is not assigned to a subscriber."

has assigned a telephone number to a subscriber. This proposal, if not supported by use of a 100 percent reliable real-time database (which does not exist), could prevent outgoing domestic call completion for consumers who are assigned newly-activated telephone numbers.

Even if such a database were to be developed, authorizing blocking of calls on this basis would result in blocking of legitimate calls. SkypeOut is a one-way outbound calling feature. Because SkypeOut is not a two-way feature – that is, SkypeOut does not enable the receipt of incoming calls – Skype users employ it without being assigned a corresponding telephone number. SkypeOut users can populate their caller ID field either with their mobile telephone number (once verified) or with a number issued to them by Skype via a separate inbound calling feature (Skype Number).[17] Most SkypeOut users, however, do not populate their caller ID field. Many retail devices and telephone services offer a feature that prevents calls lacking caller ID from ringing (some go to voice mail, others simply don't connect). The prevalent adoption of these features imposed a significant negative impact on SkypeOut call completion rates. To correct for this problem, Skype populates otherwise-unpopulated caller ID fields on SkypeOut calls with a valid telephone number allocated to Skype (and within Skype's pool of numbers available for assignment) but not assigned to a specific user. Typically, this results in the

[17] The vast majority of SkypeOut users do not have a phone number separately assigned by Skype.

caller ID being a "Skype call." If the Commission were to authorize blocking of calls allocated to a carrier but not assigned to a subscriber, it would jeopardize call completion for the majority of SkypeOut calls made to U.S. telephone numbers.

III. The Commission Should Explore Alternatives to Number-Based Call Blocking

The concept of blocking calls based upon an originating telephone number rests on the invalid assumption that a telephone number is required to make an outgoing call. A telephone number is required to receive a call from the public switched telephone network, but not to place an outgoing call to that network. Several applications, including SkypeOut, permit outbound calls to the public switched telephone network from an internet-connected device without assigning a telephone number to the calling party. If these applications are not considered during the development of rules designed to prevent caller ID fraud and illegal robocalls, such non-traditional calling applications and their underlying technology may inadvertently be swept into the category of illegal – and blocked – calls. Accordingly, as the Commission considers telephone number-based efforts to reduce illegal calls, it should remain mindful that a telephone number is not necessary to originate a call.

Further, Microsoft encourages the Commission and industry stakeholders to think about a broader range of mechanisms that could be used to prevent illegal robocalls and caller ID fraud. For example, alerting a customer in real-time to the potential for fraud with a virtual tap on the shoulder could be equally or more effective in combating

the harm ensuing from caller ID fraud without the negative risk or network reliability degradation inherent in a call blocking approach.

A Senior Software Engineer at Microsoft recently developed an approach to do just that. He was on the receiving end of an income tax scam call that unnerved him. Although he subsequently discovered through an internet search that this call was a scam, he thought it would be good to develop an automated technology to identify the likelihood that a call is a scam, and warn the called party during the call if that likelihood is high.

The technology he developed[18] could gather data including voice samples, background noise samples, caller ID area codes, the caller ID telephone number, the called party's area code, the time of the call, and some demographic information about the called party. This data could be used in a machine learning phase to identify common features in scam calls including background noises, key words being used, time of calls, etc. A user could activate the feature to pull a sample of an incoming call and, if these patterns are recognized on samples from an incoming call, the service or device could alert the called party through a vibration, a tone, or even a whisper to warn

[18] The patent application for the technology is US Patent Application No. 20170142252 and is available online at <http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220170142252%22.PGNR.&OS=DN/20170142252&RS=DN/20170142252>.

the caller to be wary of revealing any personal information or making any payments on that call. This technology has not been implemented into a commercial offering yet, but it provides a single example of how something other than call blocking can provide consumer protection benefits without negatively affecting the utility and reliability of the public switched telephone network. Such alternative approaches warrant investigation.

IV. Notice of Inquiry Matters

A. *SHAKEN Is Not Yet A Sufficiently Reliable Authentication Method*

There remains significant work to be done before SHAKEN can be implemented as a reliable authentication method and, without specifying the details, Microsoft has serious concerns about some shortcomings in its current iteration.[19] The undertaking holds sufficient promise, however, to warrant continued effort and Microsoft hopes to remain involved. It would be premature, however, for the Commission to opine on

[19] The Notice encourages the industry to implement standards when it cannot know what the standards will look like in their final form – including whether they would raise public interest concerns. *See* Notice at ¶ 32 ("The Commission recognizes that standards bodies have made significant progress on Caller ID Authentication Standards. We applaud this progress, and encourage the industry to implement these standards as soon as they are capable of doing so."). These particular standards will prevent the completion of some calls and, because they have not been finalized, their effects on the reliability of the network cannot yet be evaluated. Accordingly, Microsoft respectfully suggests that it is premature for the Commission to express its approval or encourage implementation.

whether the SHAKEN protocol could serve as the basis for the Commission to authorize industry-wide blocking of unauthenticated calls.[20]

B. *The Commission Should Not Adopt Safe Harbors*

The Commission should refrain from implementing safe harbors at this time. Safe harbors could reduce the incentive to improve and maintain precision of call blocking mechanisms. The Commission can exercise prosecutorial discretion in the early stages of any call blocking systems designed to prevent illegal robocalling and caller ID fraud. By proceeding in this manner, the Commission can avoid "gotcha" scenarios, yet maintain the ability to correct for blocking practices that prevent too many legitimate calls from reaching the called party.

V. Conclusion

Microsoft is aligned with the Commission in its commitment to battling caller ID scams and illegal robocalling. Indeed, Microsoft has been active on this matter; it is working with the Federal Trade Commission and international, federal, and state law enforcement bodies, and has pursued enforcement actions against U.S. entities, call centers in India, and fraudsters in Latin America. It has developed and implemented technological measures to deter scams that harm consumers. And it has undertaken efforts to educate consumers and remind them of ways they can protect themselves.

[20] *See id.* (seeking comment on whether, once SHAKEN is widely adopted, providers should be permitted to block calls lacking authenticated caller ID).

Microsoft emphasizes its support for the Commission's interest in eliminating caller ID scams and illegal robocalls and believes there are some worthy proposals in the Notice. If, however, the implications of implementing these proposals are not adequately vetted, the zeal in battling a problem may create new ones that are equally harmful, albeit in different ways. Call blocking, under the appropriate circumstances and conditions, may be a tool that helps to reduce caller ID scams. It cannot be denied, however, that it is an extreme approach. Therefore, Microsoft encourages an analysis that is broad in its thinking, considers all technologies and scenarios, and is deliberative before authorizing practices as extreme as call blocking.

Respectfully submitted,

MICROSOFT CORPORATION

/s/ Paula Boyd

Paula Boyd
Senior Director, Government and Regulatory Affairs
901 K Street, NW, 11th Floor
Washington, DC 20001
202.263.5946
Paula.Boyd@Microsoft.com

Gunnar Halley
Senior Attorney, CELA - Regulatory Affairs
One Microsoft Way
Redmond, WA 98052
425.703.3651
gunnarh@microsoft.com

Dated: 3 July 2017